SECTION II—REMARKS

Applicants thank the Examiner for a thorough review, and respectfully request reconsideration of the above referenced patent application for the following reasons:

Claims rejected under 35 U.S.C. § 112, second paragraph

The PTO rejected claims 1-4, 6-10, 12-14, 16, 18-19, 21, 23-26, 28-30, 32, and 34-42 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. In particular, the PTO rejected independent claims 1, 7, 13, 18, 23, 29, 34 and 39 asserting that:

> **a portion of the shared secret has already been used in a symmetric key cryptography between the terminal and the access point.** Therefore disqualifying the portion of the shared secret from use in symmetric key cryptography render[s] the claims vague and indefinite, **because the access point would not possess a qualifying shared secret to recover the scrambled user terminal certificate.**

Applicants respectfully assert that the PTO has misunderstood the manner in which the invention is practiced, and traverse the rejection. Where necessary, Applicants have provided references to appropriate paragraphs of the original specification providing support for the claimed limitations rejected by the PTO.

Moreover, Applicants respectfully point out that claims 1-4, 6-10, 12, 23-26, 28, and 34-38 were rejected under 35 U.S.C. § 112, second paragraph "because the access point [cannot] **recover the scrambled user terminal certificate**." However, these claims neither address nor recite unscrambling or "recover[ing] the scrambled user terminal certificate" upon which the PTO bases its rejection. Applicants therefore cannot address this argument with regard to claims

1-4, 6-10, 12, 23-26, 28, and 34-38, but instead address the argument only with reference to claims 13-14, 16, 18-19, 21, 29-30, 32, and 39-42 below.

Symmetric key cryptography not already used

The PTO asserts that "symmetric key cryptography" has "already been used" between the user terminal and the access point. Refer to the Office Action dated March 5, 2007, page 3 ¶ 4.

Applicants respectfully disagree. Applicants neither teach nor recite that "a portion of the shared secret has already been used in a symmetric key cryptography." To the contrary, independent claim 1 for example recites a method comprising "scrambling a user terminal certificate using a first portion of a shared secret." The claim is silent with regard to the use of symmetric key cryptography between the user terminal and the access point. Indeed, independent claim 1 expressly recites "disqualifying the first portion of the shared secret from use with symmetric key cryptography between the user terminal and the access point."

The specification likewise does not support the PTO's assertion that "a portion of the shared secret has already been used in a symmetric key cryptography between the terminal and the access point." The specification expressly states that symmetric key cryptography can be used in "**all further communication** between the UT ... and the AP," after the AP "authenticate[s] the UT 108 using a single message from the UT," but it says nothing about symmetric key cryptography "ha[ving] already been used" as the PTO asserts. Refer to paragraph 42 of the original specification.

The scrambled user terminal certificate **can** be recovered

The PTO further asserts that "the access point [cannot] recover the scrambled user terminal certificate." Refer to the Office Action dated March 5, 2007, page 3 ¶ 4.

Again, Applicants must respectfully disagree. The original specification teaches how the scrambled user terminal certificate **can** be recovered and Applicants appropriately recite how this is done in the relevant claims.

At paragraph 28 of the original specification, Applicants teach first how the user terminal certificate can be scrambled, stating that:

> **[0028]** In one embodiment, the UT certificate is scrambled using at least a **part of the shared secret** ... For example, **the designated scrambling bits of the shared secret can be used to seed a linear feedback shift register whose output can be used to scramble the UT certificate.** In one embodiment, the bits generated by the linear feedback shift register are XOR-ed with the bits of the UT certificate.

Independent claim 1, which recites in pertinent part "scrambling a user terminal certificate using a first portion of a shared secret" finds support in the above referenced paragraph. The limitation is further supported by Figure 3 which illustrates "a shared secret" at element 310, broken into sub-elements 310A, the "first portion," and 310B, the remaining portion. As can be seen from Figure 3 via broken line 308, the first portion 310A and the user terminal certificate 306 are both fed into the scramble function located at element 304 resulting in a scrambled user terminal certificate at element 302A.

With regard to the PTO's assertion that an "access point [cannot] recover the scrambled user terminal certificate," Applicants respectfully point out the pertinent teachings from paragraphs 44-45 of the original specification, stating:

> **[0044]** As described above, field 302A is generated by scrambling 304 the UT certificate 306. As shown by dotted line 308, a part 310A of the shared secret 310 is used for the scrambling 304. Secret 310A is used to initialize a linear feedback shift register. Then, the LFSR's output is XOR-ed with the UT certificate 306. This hides the UTID 312 from eavesdroppers, and makes UT tracking more difficult. **To unscramble the UT certificate 306 an AP will need to know the shared secret 310.**
>
> **[0045]** Field **302B** [the message received at an access point] **contains the shared secret 310** encrypted 320 with the AP public key. Since only the AP who possesses the private key corresponding with this public key can decrypt the shared secret 310, **only this AP can unscramble the UT certificate.**

Independent claim 13, which recites in pertinent part "unscrambling the user terminal certificate using a first portion of the decrypted shared secret" finds support in the above referenced paragraph.

Thus, independent claim 1 recites a method at a user terminal "comprising: **scrambling a user terminal certificate**" which is supported by the specification, and independent claim 13 recites a method at an access point "comprising ... **unscrambling the user terminal certificate**," which is likewise supported by the specification.

Accordingly, Applicants respectfully submit that independent claims 1 and 13 are in condition for allowance as the limitations they recite are definite, particularly pointing out and claiming the subject matter that Applicants regard as the invention, and are furthermore supported by the original specification. Independent claims 7, 23 and 34 contain similar limitations to those of independent claim 1, and therefore are also in condition for allowance. Moreover, independent claims 18, 29, and 39 contain similar limitations to those of independent claim 13, and therefore independent claims 18, 29, and 39 are likewise in condition for allowance. Finally, dependent claims 2-4, 6, 8-10, 12, 14, 16, 19, 21, 24-26, 28, 30, 32, 35-38, and 40-42, rejected by the PTO on the basis of their dependency on the aforementioned

independent base claims are in condition for allowance as the independent claims upon which they depend are in condition for allowance.

In accordance with the preceding discussion, Applicants respectfully request the PTO withdraw its rejection to claims 1-4, 6-10, 12-14, 16, 18-19, 21, 23-26, 28-30, 32, and 34-42 rejected under 35 U.S.C. § 112, second paragraph.

CONCLUSION

Given the above remarks, all claims pending in the application are in condition for allowance. If the undersigned attorney has overlooked subject matter in any of the cited references that is relevant to allowance of the claims, the Examiner is requested to specifically point out where such subject matter may be found. Further, if there are any informalities or questions that can be addressed via telephone, the Examiner is encouraged to contact the undersigned attorney at (503) 439-8778.

Charge Deposit Account

Please charge our Deposit Account No. 02-2666 for any additional fee(s) that may be due in this matter, and please credit the same deposit account for any overpayment.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: May 17, 2007

/Gregory D. Caldwell/
Gregory D. Caldwell
Attorney for Applicants
Registration No. 39,926

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles CA 90025-1030
Phone: (503) 439-8778
Facsimile: (503) 439-6073